

1 **IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

2 Application Serial No.09/757,058
3 Filing Date Jan. 8, 2001
4 InventorshipBrezak et al.
5 Applicant Microsoft Corporation
6 Group Art Unit2134
7 Examiner Tran, Ellen C.
8 Confirmation No.6566
9 Attorney's Docket No. MS1-679US
10 Title: Credential Managment

11
12 To: Honorable Commissioner for Patents
13 Alexandria, VA 22313-1450

14 From: Emmanuel A. Rivera (Tel. 509-324-9256; Fax 509-323-8979)
15 **Customer No. 22801**

16 **RESPONSE TO OCTOBER 19, 2005 NON-FINAL OFFICE ACTION**

17 Sir:

18 In response to the office action (the Action) of **October 19, 2005**, the
19 response is provided as follows:

20 Amendments to the specification begin on page 2 of this paper.

21 The listing of the claims begins on page 4 of this paper.

22 Remarks/Arguments begin on page 14 of this paper.

Amendments to the Specification

Please replace the paragraph at page 2, beginning at line 2 with the following:

A “credential” is a generic term for data used to verify the identity of an entity. An entity may be a server, a client, a service, etc. Typically, it is a user. Common forms of credentials include username/password model, X.509 Certificates, and bio-metric identification. There are two general types of credentials: Domain credentials and generic credentials.

Please replace the paragraphs at page 9, beginning at line 9 with the following:

A credential management module 152 is one such security process in the TCB 150. As its name implies, it manages the credentials of the computer 130. More specifically, it manages the credentials of each user of the computer 130.

Although not illustrated in Fig. 1, credential management module 152 may be composed multiple submodules. Some of these may be application-programming interfaces (APIs) that the applications may call to access credentials. More details about such APIs are provided in the “Exemplary Implementation employing APIs” section below. One or more other submodules may control the actual access of a user’s credentials (including reads and writes) and control the encryption and decryption of credential databases, such as databases 154a-c. Herein, this submodule may be called the “credential management submodule.”

1 Please replace the paragraph at page 9, beginning at line 22 with the
2 following:

3 Fig. 1 illustrates multiple encrypted credential databases 154a-c with a
4 graphical representation of a “user” associated with each database. This indicates
5 that each database is associated with a particular user. The credentials for each
6 user is collected and stored together within a database structure (e.g., databases
7 154a-c) associated with a specific user. That database is encrypted.

8
9 Please replace the paragraph at page 11, beginning at line 1 with the
10 following:

11 Marshaling

12
13 Marshaling is the mechanism by which a description of a non-password
14 credential can be passed to the TCB using an interface designed to support only
15 password credentials. See the marshaling APIs, described in the “Exemplary
16 Implementation employing APIs “ section below, for details of an implementation
17 that performs marshaling.